ELIZABETH CITY STATE UNIVERSITY
Asset Management Policy

1. PURPOSE

The purpose of this policy is to protect information resources and data by ensuring appropriate handling requirements are followed to prevent unauthorized use, disclosures, and theft. This policy establishes minimum guidelines for Elizabeth City State University's (ECSU) Division of Information Technology (DIT) to protect the confidentiality, integrity, and availability of ECSU information resources accessed, managed, and/or controlled by the University.

2. SCOPE

This policy applies to all ECSU employees whether full-time or part-time, paid or unpaid, temporary or permanent, volunteers, as well as to all other members of the ECSU community.

3. ACRONYMS / DEFINITIONS

Availability. The measures to which information and critical ECSU services are accessible for use when required.

Confidentiality. The measures to which confidential ECSU information is protected from unauthorized disclosure.

Information Resource. Data, information, and information systems used by ECSU to conduct ECSU operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

Information Asset. Any ECSU-owned and managed equipment used to conduct ECSU operations.

Information Security. The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.

Integrity. The measures to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of ECSU.

Principle of Least Privilege. This principle states a process will be granted only those privileges which are essential to perform its intended function.

4. POLICY

A. ASSET PROCUREMENT

Hardware And Software Procurement - All hardware and software must be procured through the ECSU Purchasing Department according to DIT standards.

Vendors Providing Mission Critical Hardware, Software, and Services - All ECSU's mission critical hardware, software and services must be purchased, rented, leased, or otherwise obtained from a trusted and well-established vendor who is able to provide both maintenance services as well as warranties.

B. ASSET INVENTORY

Assets must be identified, and an inventory of these assets must be drawn up and maintained. ECSU's Division of Information Technology (DIT) maintains an inventory of its information systems and assets. The DIT maintains an inventory of its assets that includes, but is not limited to:

i. A list of devices and personnel with access;
ii. A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding, and/or inventorying of devices);
iii. List of ECSU-Approved hardware & software;
iv. A Process to update and review the inventory on a frequent basis; and
v. Vendor/Manufacturer, device type, model, serial number, and physical location.

Asset Inventory - Technology - ECSU Information Technology Client Services prepares an annual inventory of production information systems detailing all existing production hardware, software, and communications links.

Asset Inventory Contents – Every asset recorded in the asset inventory includes, at a minimum, the following information:

i. Asset Name
ii. Asset Owner
iii. Asset Location
iv. Security Classification
v. Hardware Inventory & Specifications
vi. Software License Information
vii. Software Version Numbers
viii. Information System/Component Owners
ix. Networked components or devices, machine names and network addresses

Network and System Architecture Diagram verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component of that system.

ECSU Division of Information Technology:

i. Verifies that a current network and system architecture diagram exists for their environment(s);
ii. Maintains a current diagram that shows all data flows across systems and networks;
iii. Documents all connections, including any wireless networks and Hosted / Cloud Services; and
iv. Verifies network and system architecture diagrams include security controls employed, with sufficient detail to permit analysis and testing.

Equipment Tags - All information equipment have a unique computer-readable identifier attached to it such that physical inventories can be efficiently and regularly conducted.

C. OWNERSHIP & CLASSIFICATION

All assets and information systems maintained in the inventory are assigned ownership.

i. **Asset Ownership** - All production information assets possessed by or used by ECSU have a designated owner with ownership responsibilities clearly documented.
ii. **Security Classification** - Every ECSU asset is assigned an information security classification defining the security and recovery details for each asset type.

D. EQUIPMENT AUTHORIZATION

ECSU-Managed Devices - Personnel must not use personal computing devices to store or process ECSU information unless authorized by ECSU Information Technology Client Services. All mobile devices used for ECSU purposes must be issued or authorized by the ECSU Information Technology Client Services.

Approved Security Configuration – All information equipment issued to personnel, including personal computers, mobile devices, and smart phones, must be configured according to standards approved by ECSU Information Technology Client Services.

E. EQUIPMENT REMOVAL

Property Passes - Information systems equipment (e.g., servers, desktop computers, modems, routers) must not leave ECSU premises unless accompanied by an approved property pass and must be logged building security

Media Removal - All computer storage media leaving ECSU premises must be accompanied by a properly authorized pass and must be logged building security.

F. EQUIPMENT RETURN

Mobile devices must be returned for Decommission - All ECSU issued mobile devices, including laptops, Tablets or cell phones must be returned to ECSU Information Technology Services when no longer in use by employees or contractors.

Devices Holding Confidential Data Must Not be Resold - ECSU storage devices such as hard-drives, portable disks, tablets, electronic cameras, and cell phones which store confidential data must not be resold or recycled. These devices must be destroyed using sensitive information destruction procedures established by ECSU Information Technology Client Services.

G. DISPOSAL OF COMPUTER EQUIPMENT

Procedures governing asset management are established for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport, or surplus.

When disposing of any asset, confidential data is removed prior to disposal ECSU Information Technology Client Services must determine what type of data destruction protocol should be used for erasure.

Minimally, data must be removed using low level formatting and degaussing techniques. For media storing confidential data or Personally Identifiable Information (PII) or Protected Health Information (PHI) that is not being repurposed, disks shall be physically destroyed prior to disposal.

Information Systems Equipment Disposal - Before disposal, donation, or recycling, ECSU Information Technology Client Services will validate that confidential data or Personally Identifiable Information (PII), or Protected Health Information (PHI) has been removed. This validation process must take place before releasing such equipment.

Outsourced Data Destruction - ECSU Information Technology Client Services must verify the data specific methods of all third parties contracted for destruction of equipment containing confidential data or Personally Identifiable Information (PII) or Protected Health Information (PHI).

Inventory Of Decommissioned Computer and Network Equipment - The ECSU Information Technology Client Services must maintain an inventory of all ECSU computer and network equipment that has been taken out of commission. This inventory must also reflect all actions taken to clear memory chips, hard drives, and other storage locations.

Labeling Required - Equipment designated for surplus or other re-use must have a label affixed stating that the hard drive has been properly sanitized.

Office Machines Require Proper Disposal - All ECSU (fax, copy) machines must have their internal disk drives properly erased before disposal or replacement in accordance with destruction procedures established by ECSU Information Technology Client Services.

5. PROCEDURES

ECSU shall develop, manage, and review operating procedures to create the proper security posture for protecting ECSU information resources. Such procedures shall be periodically reviewed as required.

6. COMPLIANCE / ENFORCEMENT / SANCTIONS

Any ECSU employee or student found to have violated this policy shall be subject to disciplinary action. Sanctions will be proportionate with the severity and/or frequency of offense and can include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

7. EXCLUSIONS / EXCEPTIONS

No approved exceptions exist at this time.